

110TH CONGRESS
1ST SESSION

H. R. 964

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 8, 2007

Mr. TOWNS (for himself, Mrs. BONO, Mr. DINGELL, Mr. BARTON of Texas, Mr. RUSH, Mr. STEARNS, Mr. MARKEY, Ms. SCHAKOWSKY, Mr. BOUCHER, Mr. GORDON of Tennessee, Ms. ESHOO, Mr. STUPAK, Mr. GENE GREEN of Texas, Ms. DEGETTE, Mrs. CAPPS, Mr. DOYLE, Ms. SOLIS, Mr. GONZALEZ, Mr. INSLEE, Ms. HOOLEY, Mr. WEINER, Mr. MATHE-SON, Mr. BUTTERFIELD, Mr. HASTERT, Mr. RADANOVICH, Mr. TERRY, Mrs. MYRICK, Mr. BURGESS, and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Securely Protect Your-
5 self Against Cyber Trespass Act” or the “Spy Act”.

1 thorized user or a third party defrauded by
2 such conduct to incur charges or other costs for
3 a service that is not authorized by such owner
4 or authorized user;

5 (D) using the computer as part of an ac-
6 tivity performed by a group of computers that
7 causes damage to another computer; or

8 (E) delivering advertisements that a user
9 of the computer cannot close without undue ef-
10 fort or knowledge by the user or without turn-
11 ing off the computer or closing all sessions of
12 the Internet browser for the computer.

13 (2) Modifying settings related to use of the
14 computer or to the computer's access to or use of
15 the Internet by altering—

16 (A) the Web page that appears when the
17 owner or authorized user launches an Internet
18 browser or similar program used to access and
19 navigate the Internet;

20 (B) the default provider used to access or
21 search the Internet, or other existing Internet
22 connections settings;

23 (C) a list of bookmarks used by the com-
24 puter to access Web pages; or

1 attempts to decline the installation, the installa-
2 tion nevertheless proceeds; or

3 (B) causing such a component that the
4 owner or authorized user has properly removed
5 or disabled to automatically reinstall or reac-
6 tivate on the computer.

7 (6) Misrepresenting that installing a separate
8 component of computer software or providing log-in
9 and password information is necessary for security
10 or privacy reasons, or that installing a separate com-
11 ponent of computer software is necessary to open,
12 view, or play a particular type of content.

13 (7) Inducing the owner or authorized user to
14 install or execute computer software by misrepre-
15 senting the identity or authority of the person or en-
16 tity providing the computer software to the owner or
17 user.

18 (8) Inducing the owner or authorized user to
19 provide personally identifiable, password, or account
20 information to another person—

21 (A) by misrepresenting the identity of the
22 person seeking the information; or

23 (B) without the authority of the intended
24 recipient of the information.

1 (A) such information collection program
2 provides notice in accordance with subsection
3 (c) before execution of any of the information
4 collection functions of the program; and

5 (B) such information collection program
6 includes the functions required under sub-
7 section (d); or

8 (2) to execute any information collection pro-
9 gram installed on such a protected computer un-
10 less—

11 (A) before execution of any of the informa-
12 tion collection functions of the program, the
13 owner or an authorized user of the protected
14 computer has consented to such execution pur-
15 suant to notice in accordance with subsection
16 (c); and

17 (B) such information collection program
18 includes the functions required under sub-
19 section (d).

20 (b) INFORMATION COLLECTION PROGRAM.—

21 (1) IN GENERAL.—For purposes of this section,
22 the term “information collection program” means
23 computer software that performs either of the fol-
24 lowing functions:

tion collection program by reason of paragraph

(1)(B) shall not be considered such a program if—

(A) the only information collected by the software regarding Web pages that are accessed using the computer is information regarding Web pages within a particular Web site;

(B) such information collected is not sent to a person other than—

(i) the provider of the Web site accessed; or

(ii) a party authorized to facilitate the display or functionality of Web pages within the Web site accessed; and

(C) the only advertising delivered to or displayed on the computer using such information is advertising on Web pages within that particular Web site.

(c) NOTICE AND CONSENT.—

(1) IN GENERAL.—Notice in accordance with this subsection with respect to an information collection program is clear and conspicuous notice in plain language, set forth as the Commission shall provide, that meets all of the following requirements:

1 information to display advertising on your
2 computer. Do you accept?''.

3 (C) The notice provides for the user—

4 (i) to grant or deny consent referred
5 to in subsection (a) by selecting an option
6 to grant or deny such consent; and

7 (ii) to abandon or cancel the trans-
8 mission or execution referred to in sub-
9 section (a) without granting or denying
10 such consent.

11 (D) The notice provides an option for the
12 user to select to display on the computer, before
13 granting or denying consent using the option
14 required under subparagraph (C), a clear de-
15 scription of—

16 (i) the types of information to be col-
17 lected and sent (if any) by the information
18 collection program;

19 (ii) the purpose for which such infor-
20 mation is to be collected and sent; and

21 (iii) in the case of an information col-
22 lection program that first executes any of
23 the information collection functions of the
24 program together with the first execution
25 of other computer software, the identity of

1 such notice shall provide the option under subpara-
2 graph (D) of paragraph (1) of this subsection with
3 respect to each such information collection program.

4 (3) CHANGE IN INFORMATION COLLECTION.—If
5 an owner or authorized user has granted consent to
6 execution of an information collection program pur-
7 suant to a notice in accordance with this subsection:

8 (A) IN GENERAL.—No subsequent such
9 notice is required, except as provided in sub-
10 paragraph (B).

11 (B) SUBSEQUENT NOTICE.—The person
12 who transmitted the program shall provide an-
13 other notice in accordance with this subsection
14 and obtain consent before such program may be
15 used to collect or send information of a type or
16 for a purpose that is materially different from,
17 and outside the scope of, the type or purpose
18 set forth in the initial or any previous notice.

19 (4) REGULATIONS.—The Commission shall
20 issue regulations to carry out this subsection.

21 (d) REQUIRED FUNCTIONS.—The functions required
22 under this subsection to be included in an information col-
23 lection program that executes any information collection
24 functions with respect to a protected computer are as fol-
25 lows:

1 for the exclusive purpose of identifying the pro-
2 gram, or a statement or other information suffi-
3 cient to clearly identify the program.

4 (B) EXEMPTION FOR EMBEDDED ADVER-
5 TISEMENTS.—The Commission shall, by regula-
6 tion, exempt from the applicability of subpara-
7 graph (A) the embedded display of any adver-
8 tisement on a Web page that contempora-
9 neously displays other information.

10 (3) RULEMAKING.—The Commission may issue
11 regulations to carry out this subsection.

12 (e) LIMITATION ON LIABILITY.—A telecommuni-
13 cations carrier, a provider of information service or inter-
14 active computer service, a cable operator, or a provider
15 of transmission capability shall not be liable under this
16 section to the extent that the carrier, operator, or pro-
17 vider—

18 (1) transmits, routes, hosts, stores, or provides
19 connections for an information collection program
20 through a system or network controlled or operated
21 by or for the carrier, operator, or provider; or

22 (2) provides an information location tool, such
23 as a directory, index, reference, pointer, or hypertext
24 link, through which the owner or user of a protected
25 computer locates an information collection program.

1 protected computers shall be treated as a single
2 violation; and

3 (B) any single action or conduct that vio-
4 lates more than one paragraph of section 2(a)
5 shall be considered multiple violations, based on
6 the number of such paragraphs violated.

7 (c) REQUIRED SCIENTER.—Civil penalties sought
8 under this section for any action may not be granted by
9 the Commission or any court unless the Commission or
10 court, respectively, establishes that the action was com-
11 mitted with actual knowledge or knowledge fairly implied
12 on the basis of objective circumstances that such act is
13 unfair or deceptive or violates this Act.

14 (d) FACTORS IN AMOUNT OF PENALTY.—In deter-
15 mining the amount of any penalty pursuant to subsection
16 (a) or (b), the court shall take into account the degree
17 of culpability, any history of prior such conduct, ability
18 to pay, effect on ability to continue to do business, and
19 such other matters as justice may require.

20 (e) EXCLUSIVENESS OF REMEDIES.—The remedies
21 in this section (including remedies available to the Com-
22 mission under the Federal Trade Commission Act) are the
23 exclusive remedies for violations of this Act.

24 (f) EFFECTIVE DATE.—To the extent only that this
25 section applies to violations of section 2(a), this section

1 such monitoring or interaction is for network or
2 computer security purposes, diagnostics, technical
3 support, or repair, or for the detection or prevention
4 of fraudulent activities; or

5 (2) a discrete interaction with a protected com-
6 puter by a provider of computer software solely to
7 determine whether the user of the computer is au-
8 thorized to use such software, that occurs upon—

9 (A) initialization of the software; or

10 (B) an affirmative request by the owner or
11 authorized user for an update of, addition to, or
12 technical service for, the software.

13 (c) GOOD SAMARITAN PROTECTION.—No provider of
14 computer software or of interactive computer service may
15 be held liable under this Act on account of any action vol-
16 untarily taken, or service provided, in good faith to remove
17 or disable a program used to violate section 2 or 3 that
18 is installed on a computer of a customer of such provider,
19 if such provider notifies the customer and obtains the con-
20 sent of the customer before undertaking such action or
21 providing such service.

22 (d) LIMITATION ON LIABILITY.—A manufacturer or
23 retailer of computer equipment shall not be liable under
24 this Act to the extent that the manufacturer or retailer
25 is providing third party branded computer software that

1 strued to limit the enforcement of any State
2 consumer protection law by an Attorney Gen-
3 eral of a State.

4 (3) PROTECTION OF CERTAIN STATE LAWS.—

5 This Act shall not be construed to preempt the ap-
6 plicability of—

7 (A) State trespass, contract, or tort law; or

8 (B) other State laws to the extent that
9 those laws relate to acts of fraud.

10 (b) PRESERVATION OF FTC AUTHORITY.—Nothing
11 in this Act may be construed in any way to limit or affect
12 the Commission's authority under any other provision of
13 law, including the authority to issue advisory opinions
14 (under part 1 of volume 16 of the Code of Federal Regula-
15 tions), policy statements, or guidance regarding this Act.

16 SEC. 7. ANNUAL FTC REPORT.

17 For the 12-month period that begins upon the effec-
18 tive date under section 12(a) and for each 12-month pe-
19 riod thereafter, the Commission shall submit a report to
20 the Congress that—

21 (1) specifies the number and types of actions
22 taken during such period to enforce section 2(a) and
23 section 3, the disposition of each such action, any
24 penalties levied in connection with such actions, and

1 siders necessary and appropriate, including treatment of
2 cookies under this Act or other laws.

3 (b) DEFINITION.—For purposes of this section, the
4 term “tracking cookie” means a cookie or similar text or
5 data file used alone or in conjunction with one or more
6 Web sites to transmit or convey, to a party other than
7 the intended recipient, personally identifiable information
8 of a computer owner or user, information regarding Web
9 pages accessed by the owner or user, or information re-
10 garding advertisements previously delivered to a computer,
11 for the purpose of—

12 (1) delivering or displaying advertising to the
13 owner or user; or

14 (2) assisting the intended recipient to deliver or
15 display advertising to the owner, user, or others.

16 (c) EFFECTIVE DATE.—This section shall take effect
17 on the date of the enactment of this Act.

18 **SEC. 9. FTC REPORT ON INFORMATION COLLECTION PRO-**
19 **GRAMS INSTALLED BEFORE EFFECTIVE**
20 **DATE.**

21 Not later than the expiration of the 6-month period
22 that begins on the date of the enactment of this Act, the
23 Commission shall submit a report to the Congress on the
24 extent to which there are installed on protected computers
25 information collection programs that, but for installation

1 602 of the Communications Act of 1934 (47 U.S.C.
2 522).

3 (2) COLLECT.—The term “collect”, when used
4 with respect to information and for purposes only of
5 section 3(b)(1)(A), does not include obtaining of the
6 information by a party who is intended by the owner
7 or authorized user of a protected computer to receive
8 the information or by a third party authorized by
9 such intended recipient to receive the information,
10 pursuant to the owner or authorized user—

11 (A) transferring the information to such
12 intended recipient using the protected com-
13 puter; or

14 (B) storing the information on the pro-
15 tected computer in a manner so that it is acces-
16 sible by such intended recipient.

17 (3) COMPUTER; PROTECTED COMPUTER.—The
18 terms “computer” and “protected computer” have
19 the meanings given such terms in section 1030(e) of
20 title 18, United States Code.

21 (4) COMPUTER SOFTWARE.—

22 (A) IN GENERAL.—Except as provided in
23 subparagraph (B), the term “computer soft-
24 ware” means a set of statements or instructions
25 that can be installed and executed on a com-

1 (8) DISABLE.—The term “disable” means, with
2 respect to an information collection program, to per-
3 manently prevent such program from executing any
4 of the functions described in section 3(b)(1) that
5 such program is otherwise capable of executing (in-
6 cluding by removing, deleting, or disabling the pro-
7 gram), unless the owner or operator of a protected
8 computer takes a subsequent affirmative action to
9 enable the execution of such functions.

10 (9) INFORMATION COLLECTION FUNCTIONS.—
11 The term “information collection functions” means,
12 with respect to an information collection program,
13 the functions of the program described in subsection
14 (b)(1) of section 3.

15 (10) INFORMATION SERVICE.—The term “infor-
16 mation service” has the meaning given such term in
17 section 3 of the Communications Act of 1934 (47
18 U.S.C. 153).

19 (11) INTERACTIVE COMPUTER SERVICE.—The
20 term “interactive computer service” has the meaning
21 given such term in section 230(f) of the Communica-
22 tions Act of 1934 (47 U.S.C. 230(f)).

23 (12) INTERNET.—The term “Internet” means
24 collectively the myriad of computer and tele-
25 communications facilities, including equipment and

1 (vii) Any access code, password, or ac-
2 count number, other than an access code
3 or password transmitted by an owner or
4 authorized user of a protected computer to
5 the intended recipient to register for, or
6 log onto, a Web page or other Internet
7 service or a network connection or service
8 of a subscriber that is protected by an ac-
9 cess code or password.

10 (viii) Date of birth, birth certificate
11 number, or place of birth of an individual,
12 except in the case of a date of birth trans-
13 mitted or collected for the purpose of com-
14 pliance with the law.

15 (B) RULEMAKING.—The Commission may,
16 by regulation, add to the types of information
17 described in subparagraph (A) that shall be
18 considered personally identifiable information
19 for purposes of this Act, except that such addi-
20 tional types of information shall be considered
21 personally identifiable information only to the
22 extent that such information allows living indi-
23 viduals, particular computers, particular users
24 of computers, or particular email addresses or

1 made available), which Web pages have any of the
2 following characteristics:

3 (A) A common domain name.

4 (B) Common ownership, management, or
5 registration.

6 **SEC. 12. APPLICABILITY AND SUNSET.**

7 (a) **EFFECTIVE DATE.**—Except as specifically pro-
8 vided otherwise in this Act, this Act shall take effect upon
9 the expiration of the 12-month period that begins on the
10 date of the enactment of this Act.

11 (b) **APPLICABILITY.**—Section 3 shall not apply to an
12 information collection program installed on a protected
13 computer before the effective date under subsection (a) of
14 this section.

15 (c) **SUNSET.**—This Act shall not apply after Decem-
16 ber 31, 2013.

○